REMARKS

Claims 2-4, 8-14 and 16-23 remain in this application, with Claims 1, 5-7 and 15 cancelled and Claims 2-4, 8-11, 13 and 16-20 amended. The Applicants respectfully request, pursuant to 37 C.F.R. § 1.116(b), that the foregoing amendments be entered.

The Applicants would like to thank the Examiner for conducting a telephonic interview on November 10, 2003. During this interview, the breadth of the Holtzman et al. disclosure was discussed, as was the Applicants' position that Holtzman does not disclose the limitations set forth in at least independent Claim 21 of the present application. The interview concluded without any agreement being reached.

Because Claims 1-23 of the present application have been twice rejected, and because an agreement cannot be reached as to the breadth of Holtzman's disclosure, the Applicants, pursuant to 37 C.F.R. § 1.191, are hereby filing a Notice of Appeal (enclosed), appealing the rejections of Claims 2-4, 8-14 and 16-23. In an effort to place the claims in better form for consideration on appeal, and pursuant to 37 C.F.R. § 1.116(b), Claims 1, 5-7 and 15 have been cancelled without prejudice, and Claims 2-4, 8-11, 13 and 16-20 have been amended to either independent form (Claims 2, 9 and 16) or to depend from the same (Claims 3-4, 8, 10-11, 13 and 17-20).

It should be appreciated that the Applicants have cancelled Claims 1, 5-7 and 15 to reduce the issues presented on appeal, and reserve the right to re-file the same in a continuing application. It should further be appreciated that, in amending Claims 2, 9 and 16 to independent form, language that was considered unnecessary or redundant was removed. For example, prior to the present amendment, independent Claim 1 provided, in part, that (i) both data and information be stored on the RFID tag and that (ii) the information be communicated in accordance with the data, and Claim 2 (which depended from Claim 1) provided that (iii) the data further included an address of a particular destination system and that (ii) the information be communicated to the destination system. Therefore, to alleviate confusion, and because communicating

information in accordance with data stored on the RFID tag is broader than (and unnecessary in light of) communicating information to the destination system as identified by the data, Claim 2 (as presently amended) includes language directed toward the latter (i.e., the "in accordance with" language is replaced by "to said destination system."

In the Office Action dated July 16, 2003, the Examiner rejected Claims 1-11 and 15-23 under 35 U.S.C. § 102(e) as being anticipated by Holtzman. On page 7 of this Office Action (i.e., with respect to Claim 21), the Examiner stated that the Holtzman RFID tag stores "a unique digital identifier, a protocol identifier, and at least a destination address identifier." 7/16/03 Office Action, p. 7 (internal citations omitted). While the Applicants agree that Holtzman discloses an RFID tag that stores a unique identifier (see e.g., Applicants' May 29, 2003 response, pp. 10-11), the Applicants respectfully disagree that Holtzman discloses an RFID tag that stores "a protocol identifier" or "a destination address identifier."

As stated in Applicants' May 29, 2003 response, Holtzman discloses a system and method of using a database application and data stored on an RFID tag to determine a user's access criteria to network information. Specifically, an RFID reader is used to interrogate (i.e., read) an RFID tag. In response, the RFID tag provides the RFID reader with unique identification information. Col. 3, lines 3-7; col. 9, lines 59-62. The RFID reader then provides this information to a database application to determine the user's access criteria (i.e., what network information the user has access to). Col 5, lines 6-14. The database application, or more particularly a dispatch module in communication with the database application (see Figure 2, ref. no. 82), performs at least one action in accordance with the user's access criteria (e.g., permitting the user to resume a previous session, loading a particular web page, loading a filter program, etc.). See e.g., col. 5, lines 21-28 and lines 45-63; col. 6, lines 25-30; col. 10, lines 45-49; and col. 12, lines 27-35. Thus, Holtzman discloses (i) retrieving unique identification information from an RFID tag, (ii) providing the received information to an external

database application, (iii) using information stored on the external database application to determine the user's access criteria, and (iv) instructing a dispatch module to perform at least one action in accordance with the user's access criteria.

In an alternate embodiment, Holtzman further discloses providing reader identification information together with the unique identification information to the database application. Col. 5, lines 11-20. This enables the database application to determine access criteria in response to a particular user (or unique ID info.) **and** a particular location (or reader ID info.). Col. 13, line 64 – col. 14, line 24. For example, a user located at an airport may receive different information than if the user were located at work.

In contradistinction, the present invention (as defined by Claim 21) provides storing a protocol identifier and/or a destination identifier on the RFID tag. This allows information stored on the RFID tag to be transmitted according to the protocol identified (e.g., in a particular format, to a particular application, etc.) and/or to the destination identified. In other words, the present invention enables the RFID reader to route information stored on the RFID tag directly in accordance with data stored on the RFID tag. This is contrary to Holtzman, which further requires the use of a database application, or an external database.

In support of her assertion that Holtzman discloses an RFID tag that stores "a protocol identifier," the Examiner cited col. 3, lines 40-56 and col. 7, line 59 – col. 9, line 42. These cited sections, however, do not support such a proposition. Instead they are directed toward a method of communicating with different RFID tags. For example, col. 3, lines 40-56 provide that Manchester encoding is used to encode data that is transmitted from Marin and Philips RFID tags, and col. 7, line 59 – col. 8, line 67 provide that two state machines (i.e., a low-level state machine and a high-level state machine) can be used to decode the transmitted information. See e.g., col. 9, lines 38-42 ("This dual state machine implementation allows the system to interpret different types of tags. The low-level state machine initializes the Manchester decoder as appropriate for that

tag, and then the Manchester decoder ... interprets the data."). These sections are completely unrelated to the storage of a "protocol identifier" on an RFID tag, and fail to disclose a "protocol identifier corresponding to a protocol defining an application-specific data format" (see Claim 21) and "communicating information regarding said at least one RFID tag formatted in accordance with said protocol" (see Claim 9).

In support of her assertion that Holtzman discloses an RFID tag that stores "a destination identifier," the Examiner cited col. 3, line 57 – col. 4, line 17; col. 4, lines 33-35; col. 6, lines 11-14; col. 9, lines 30-32 and lines 55-62; col. 11, lines 15-55; and col. 12, lines 28-36 and lines 55-58. These sections, however, do not disclose the storage of a destination identifier on a RFID tag, but the storage of access criteria on a database. For example, the bottom of column 3 provides that "the computer 10 is ... connected to a computer network 25," and that "the destination address or name of the destination node is supplied to the TCP/IP software running on the computer 10" in order to establish a connection with a server via the network. Furthermore, the top of column 4 provides that "each token is associated with one of the servers, so that a token causes the computer to establish a connection with, and communicate with, one of the servers." What these two passages fail to disclose is who supplies the destination address (i.e., where is it stored) and how does the token cause the computer to establish a connection with a server.

The following column, however, provides that an identifier is received from an RFID tag and a database is consulted to determine access criteria. In other words, "upon receipt of an identifier, the dispatch module 82 queries the database 85 to locate the corresponding access criterion and any other stored information relating to the identifier, and takes appropriate action." Col. 5, lines 11-14. In one embodiment, "a web browser 80 [is] running as an active application process on computer 10" and "the dispatch module 82 obtains from the database 85 a URL associated with the received identifier, and causes the web browser 80 to connect to the referenced server and download a specified web page." Col. 5, lines 21-26. From this it is clear that the

"destination address" is stored on the database (and not on the RFID tag) and the RFID tag (or token) causes the computer to establish a connection with a server by transmitting an identifier (i.e., unique identifying information) that is linked to a destination address stored on the database. Not only does the RFID reader of the present invention, as defined by Claim 2, not require the use of an external application to identify a destination address, but such applications are considered to be a drawback of the prior art. See Application, pp. 2-3 ("The use of a software application to provide the routing functions necessarily limits the flexibility of the network application that use the collected information. It would be desirable to provide an automated data collection system in which the RFID interrogator can convey collected information to different locations, computers and/or software application based on the information content of the RFID transponder.").

The remaining citations are also unrelated to the present invention. For example, col. 6, lines 11-14 and col. 9, lines 30-32, disclose that "other information" can be stored on, or retrieved from, the RFID tag. This "other information", however, is subsequently defining as being "user-specific information such as a username, password, [and] PIN." Col. 9, lines 55-62. This "other information" is never defined as being, or including, a destination identifier.

Similarly, col. 11, lines 15-55 merely disclose how the "access information" can be used to retrieve website or email information, and are unrelated to the storage of a destination identifier on an RFID tag. According to Holtzman, "the access criteria is determined from the token identifier based on information stored in the first node, for example a list, table, or database. ... The first node performs a lookup in such list, table, or database, and determines an access criterion based on the token identifier and any such other information." Col. 9, line 62 – col. 10, line 3. The first node can then be connected to a second node in response to the access criterion by "running or launching a software or hardware application on the first node that uses some part or all of the access criterion to connect to the second node." Col. 11, lines 15-21. This may

include "providing the access criteria to a web browser or other similar software that initiates a connection to the second node" (col. 11, lines 22-40) or "providing access criterion to an electronic mail application running on the first node that initiates a connection to the second node" (col. 11, lines 41-55).

While Holtzman discloses that the RFID tag can be used to retrieve a specific file or document (as oppose to website or email information), it claims to do so "through the operation of the method just described" (i.e., through the use of unique identification information and a database application). Col. 12, lines 28-36.

Finally, col. 12, lines 55-58 merely provides that access criterion can be determined from (i) information that identifies the RFID tag or (ii) information that identifies both the RFID tag and the RFID reader. In other words, access to information can be based either on the user's identity or on both the user's identify and the user's location.

From this it is clear that Holtzman fails to disclose the storage of a "destination identifier" on a RFID tag, or more particularly, the storage of a "destination address identifier corresponding to identifying an end destination for the stored data values" (see Claim 21), "detecting data loaded in said at least one designated field of a memory of said at least one RFID tag, wherein said data includes an address of a particular destination system" (see Claim 2), or "receiving information stored in memory of said RFID tag including identifying data loaded in at least one designated memory field of said RFID tag, wherein said identifying data defines an address of a destination system" (see Claim 16). Therefore, because Holtzman fails to disclose at least the storage of a protocol identifier and/or a destination identifier on an RFID tag, it is the Applicants' position that Claims 2-4, 8-14 and 16-23 are in condition for allowance.

Therefore, enclosed herewith is a Notice of Appeal, appealing the rejections of Claims 2-4, 8-14 and 16-23. To the extent necessary, Applicants petition the Commissioner for a one-month extension of time, extending to November 17, 2003, the period for response to the Office Action dated July 16, 2003. Accordingly, and pursuant

to 37 C.F.R. § 1.17 (a)(1) and (b), a check in the amount of $440 is enclosed for the aforementioned (and enclosed) Petition for Extension of Time and the Notice of Appeal, respectively. The Commissioner is authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,

Date: November 17, 2003

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000